IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA,	)	CASE NO.: 1:21CR226
	)	
Plaintiff,	)	JUDGE CHRISTOPHER A. BOYKO
	)	
v.	)	
	)	
DAVIS LU,	)	GOVERNMENT'S OPPOSITION
	)	TO DEFENDANT DAVIS LU'S
Defendant.	)	MOTION FOR NEW TRIAL

Now comes the United States of America, by and through Carol M. Skutnik, Acting United States Attorney; Daniel J. Riedl and Brian S. Deckert, Assistant United States Attorneys, and Candina S. Heath, Senior Counsel, Department of Justice Computer Crime and Intellectual Property Section, and hereby opposes Defendant Davis Lu's motion for new trial. (R. 108: Motion, PageID 2734-56). Lu fails in his motion to establish (1) that the email alert notifications contained in Exhibits 13A and 13B constituted new evidence; (2) that they could not have been discovered earlier; (3) that they were material, and not merely cumulative or impeaching; and (4) when considering the overwhelming evidence of guilt presented during the case-in-chief, that precluding the admission of Exhibits 13A and 13B would likely have resulted in an acquittal.

I. Summary of Government's Response

Lu cannot establish that the interests of justice warrant a new trial. Contrary to Lu's claims of "unfair surprise," "trial by ambush," and "misrepresentations by the government," (*Id.,* PageID 2737, 2744, 2747) the facts demonstrate the following:

A. No discovery violation occurred; Lu had pretrial access to the data he now claims was newly discovered. Rebuttal Exhibit 13A, prepared for and presented during the Government's rebuttal testimony, is comprised of six automated email alerts found in Lu's work Outlook

account. The government believes it did provide Lu's emails to the defense but acknowledges that it has been unable to locate documentation proving that a copy was provided. (*See* Attachment A). Even if not directly sent, the materials were available for the defense's review and the defense knew or should have known that the government possessed the materials. More than four years before trial, the government provided the defense with FBI reports and a subpoena documenting the government's request for Lu's emails and the fact that the records were received. Additionally, seven months prior to trial, the Government produced Exhibit 13 to the defense. That exhibit consisted of six email alerts received by Lu that were substantially identical in format and substance to Rebuttal Exhibit 13A but from different days. It is unreasonable to believe that the defense would not have then known that the government was in possession of emails other than the six reflected in Exhibit 13.

B. The government did not violate its disclosure obligations under Rule 16; The materials in Exhibit 13A and 13B were neither introduced during the government's case in chief nor material to the defense. The Sixth Circuit has held that:

> [I]nformation which does not counter the government's case or bolster a defense is not material "merely because the government may be able to use it to rebut a defense position." Rather, there must be an indication that pre-trial disclosure would have enabled the defendant to "alter the quantum of proof in his favor," not merely that a defendant would have been dissuaded from proffering easily impeachable evidence.
>
> *United States v. Lykins*, 428 F. App'x. 621, 624 (6th Cir. 2011) (internal citations omitted).

The allegedly undisclosed data was inculpatory. Lu's argument, in essence, is that he would not have offered perjured testimony if he knew evidence of his lies existed. That falls outside of the Sixth Circuit's definition of materiality under Rule 16. As the Sixth Circuit explained, "a Rule 16 violation cannot be sustained based merely on an argument that disclosure would have

resulted in reconsideration of Lu's decision to testify or formulation of a more effective defense strategy." *Id.* 624-25.

C. Exhibit 13A and 13B are not SiteScope Records. Lu's allegations regarding the government's misrepresentations are based on a mistaken belief that Exhibit 13A, Exhibit 13B, and the underlying data are SiteScope records. During discovery, the government accurately represented to the defense what data was and was not available. At no point did the government represent to the defense that the automated email alert notification data underlying Exhibits 13, 13A, and 13B was not available. The government accurately informed Lu of what SiteScope records were available and provided them to him.

D. Rebuttal evidence is not material when used to refute perjurious testimony. Even before rebuttal, the testimony elicited, and evidence produced during the case-in-chief had already inflicted considerable damage on Lu's credibility. The rebuttal evidence presented by the government was only introduced to refute Lu's perjurious testimony and did not preclude Lu from pursuing the defenses he selected.

II. Background

A. Procedural History

A grand jury indicted Lu on April 1, 2021, with one count of Intentionally Damaging Protected Computers, in violation of 18 U.S.C. §§ 1030(c)(4)(A)(i)(I), (c)(4)(A)(i)(VI) and (c)(4)(B)(i). (R. 1: Indictment, PageID 1). On March 7, 2025, following an eight-day trial, a jury found Lu guilty and returned special verdicts that, "The offense caused damage to ten (10) or more protected computers during a one (1)-year period;" and "The offense caused loss to one or more persons during a one (1)-year period aggregating at least $5,000 in value. (R. 81: Verdict,

PageID 818). On May 12, 2025, Lu filed his motion for new trial. (R. 108: Motion, PageID 2734-56).

B. Statement of Facts

1. Background and Investigation

Between 2007 and 2019, Lu was a computer programmer with the Eaton corporation. (R. 92: Transcript, PageID 1334-35). As an Eaton employee, Lu wrote and deployed computer code that ran on the Electrical instance of Enovia, a platform used by a variety of Eaton employees and customers to store engineering design information and manage the process of making changes to the designs. (*Id.,* PageID 1314). Unbeknownst to his employer, Lu also developed multiple pieces of malicious code, which he deployed on Eaton's network. Lu used this malicious code to cause a series of server disruptions in August and September of 2019 in which Eaton's servers would "hang" or become unresponsive at random intervals. (*Id.,* PageID 1358-59). Following Lu's termination on October 4, 2019, the server disruptions ceased but were replaced by an even more serious problem when IsDLEnabledInAD, another instance of malicious code written and deployed by Lu, denied access to all users when Lu's employee ID was removed from the active employee directory. (R. 92: Transcript, PageID 1428-32). An FBI investigation followed, and agents executed a search warrant at Lu's residence on October 3, 2019. (R. 95: Transcript, PageID 1920-22). Lu was interviewed on October 7, 2019, and admitted that he wrote two of the pieces of malicious code, ChangLin and emxTemp. (*Id.,* PageID 1923-26).

2. Discovery Process

While the investigation continued, the government and Lu's counsel engaged in plea negotiations. To facilitate these discussions, the government provided Lu with a copy of the

FBI's investigative file as early as May 28, 2020. (*See* Attachment B). It was at this time that the government believes it provided a copy of Lu's emails to defense counsel however, as discussed above, it has been unable to locate documentation explicitly referencing this disclosure. The government next provided computer logs in September of 2020 and offered that "we do have additional logs so please let me know if there are specific materials that you believe would assist in plea negotiations." (*See* Attachment C). The negotiations failed to reach an agreement, and the grand jury indicted Lu on April 1, 2021. (R. 1: Indictment, PageID 1).

Following his indictment, a lengthy discovery process began which involved dozens of emails between the parties and other entities including Eaton Corporation and Dassault, the developer of the Enovia platform. Over the course of four years, the government made approximately 20 discovery disclosures via wallet drive, hard drive, and a file sharing system. Throughout the discovery process, the government made efforts to not only comply with its discovery obligations, but to assist the defense in obtaining additional records and information that were not in the government's possession.

3. *SiteScope records*

On January 13, 2022, the Government received a letter from Lu's previous counsel requesting seven (7) categories of records, including Item 6, "Electrical Enovia server restart logs from *SiteScope* from January 1, 2019, to December 31, 2019, including any/all email notifications sent to users," for examination by the defense's expert. (Emphasis added) (*See* Attachment D). This letter was one of four such requests for Eaton-held records not possessed by the government. Although the government undertook to serve as an intermediary to procure these records, thereby aiming to obviate the issuance of a Criminal Rule 17 subpoena by the

defense, Lu nonetheless found it necessary to issue a subpoena directly to Eaton for the aforementioned documentation. (*See* R. 108-2: Def. Ex. E, PageID 2788-89).

On April 14, 2022, the government provided to the defense the entirety of the SiteScope records it received from Eaton. (*See* Attachment E). At the time, Eaton only had three months of SiteScope logs still in its possession due to an automatic purge. (*See* Attachment F). A five-page sample of the approximately 116 files totaling 12.8MB of data is attached. (*See* Attachment G). As Attachment G demonstrates, rebuttal Exhibits 13A and 13B are distinct from these SiteScope records; they are not SiteScope records themselves. Instead, the data underlying 13B and from which Exhibit 13A was sourced represent automated email alert notifications of server issues generated by an Enovia application, not logs of server restarts from SiteScope.

Lu's Rule 17 trial subpoena to Eaton requested a host of documents, including the same SiteScope records mentioned above. Eaton responded to the request through counsel and indicated that the documents were no longer in their possession. (*See* R. 108-2: Def. Ex. F, PageID 2791). Jason Koler, the Eaton employee who assisted in the collection of documents responsive to Lu's requests during discovery, provided: "After reviewing Exhibits 13 and 13A, I have concluded that the exhibits are not SiteScope records. Instead, Exhibits 13 and 13A are email notifications of an issue with a server." (Attachment H).

4. Defense Issues with Discovery

Given the breadth of discovery in this matter, the discovery process included technological and logistical challenges. For example, on April 27, 2022, the Defense sent a letter requesting more documents and assistance with opening or viewing item 6. (*See* Attachment I). On April 28, 2022, the Government sent item 6 again to the Defense on a drive. (*See* Attachment J). On June 10, 2022, the Government sent documents responsive to the April 27, 2022, letter

from Defense via USAfx and noted that defense counsel was no longer active in the USAfx system. (*See* Attachment K). On July 15, 2022, the Defense sent an email asking for the discovery to be uploaded again to USAfx so that he could review it. USAfx is not intended to be a file storage application, but rather a file delivery application. If a user does not download documents placed into USAfx within 90 days, they are removed from the file server. Defense indicated that he only needed the discovery covered by the protective order placed on USAfx. (*See* Attachment L).

On August 17, 2022, the Defense requested the previously disclosed discovery be placed on USAfx again as the defense expert needed access to it. The discovery was again uploaded to USAfx. (*See* Attachment M). On November 2, 2022, the Government provided a wallet drive containing additional FBI reports and attachments, including the Eaton subpoena and FBI reports detailing the receipt of Lu's emails, discussed more fully below. (*See* Attachment N). The above examples illustrate the government's good faith efforts to not only comply with its discovery obligations, but to make additional efforts to ensure that Lu's counsel had full access to the materials in this case.

Lu's attorneys were provided clear evidence that the Government had obtained Lu's Eaton emails. If they were unable to locate them in discovery, they need only have asked and a copy would have been provided. The Government fully believed that the emails had been provided, which is evidenced by 1) the disclosure of the FBI-302s describing the fact that the emails were obtained, and 2) the Government's disclosure of a selection of the emails in Exhibit 13 months before trial.

5. Lu's Eaton emails.

On November 2, 2022, the Government provided a discovery drive to defense containing the FBI's investigative file for this matter. (*See* Attachment N). Near the beginning of the investigative file, Serial 2 was an FBI 302 detailing the issuance of a subpoena to Eaton for records relating to Lu's employment with Eaton and specifically requesting all of the emails from his Eaton account.

> On September 23, 2019, SA Monica Hantz served a Federal Grand Jury Subpoena on Eaton. The subpoena was served in person at 1000 Eaton Boulevard, Beachwood, Ohio. The subpoena requested responsive documents related to the following:
>
> Any all records associated with Eaton employee Davis Lu aka E Lu, date of birth December 22, 1969. The records return should include but is not limited to Davis Lu aka E Lu personnel file and records of payment including direct deposit information. Additionally, please provide all emails to and from Mr. Lu's Eaton email account.
>
> A copy of the subpoena will be maintained in the 1A section of this communication.

(emphasis added) (Attachment O).

Following Serial 2 was a copy of the subpoena itself:

AO110 (Rev. 04/07) Subpoena to Testify Before Grand Jury

UNITED STATES DISTRICT COURT

Northern DISTRICT OF Ohio

TO:

Eaton Corporation
1000 Eaton Blvd
Beachwood, OH 44122

SUBPOENA TO TESTIFY BEFORE GRAND JURY

SUBPOENA FOR:
☐ PERSON ☑ DOCUMENT(S) OR OBJECT(S)

YOU ARE HEREBY COMMANDED to appear and testify before the Grand Jury of the United States District Court at the place, date, and time specified below.

PLACE	COURTROOM
Carl B. Stokes U.S. Courthouse 801 W. Superior Avenue Cleveland, Ohio 44113	Grand Jury Suite, Lower Level 1
	DATE AND TIME 10/15/2019 at 9:00 am

YOU ARE ALSO COMMANDED to bring with you the following document(s) or object(s):*

Please provide: Any all records associated with Eaton employee Davis Lu aka E Lu, date of birth December 22, 1969. The records return should include but is not limited to Davis Lu aka E Lu personnel file and records of payment including direct deposit information. Additionally, please provide all emails to and from Mr. Lu's Eaton email account.

(Attachment P)

And following that was another FBI 302 noting receipt of the records requested in the subpoena:

On September 23, 2019, SA Monica Hantz received a response from Matthew Coberly, Eaton Corporation. The response was provided pursuant to a Federal Grand Jury Subpoena served on Eaton on the same day, requesting records associated to Eaton employee DAVIS LU aka E LU.

The response will be maintained in the 1A section of the investigative file.

(Attachment Q).

On July 19, 2024, before the initial July 2024 trial date, the Government provided the defense with its case-in-chief trial exhibits, including Exhibit 13. (*See* Attachments R and S). This exhibit was substantially identical in format and substance to the rebuttal Exhibit 13A, and contained some of the very content Lu now claims he never received. Lu even used this material

in his direct examination PowerPoint presentation. (*See* Attachment T). Defense counsel never inquired about the documents in Attachments O, P, or Q), or about the origins of the emails that were used to create Exhibit 13. Lu's attorneys had ample notice dating back to November 2, 2022, that the emails were in the Government's possession and available for copy or inspection. On August 10, 2023, the Government sent several documents to the Defense, including a spreadsheet that documented that Lu was logged on and active on August 4, 2019. (*See* Attachment U). On July 19, 2024, the Government sent its Jencks material and trial exhibits, including Exhibit 13, to the Defense via USAfx. (*See* Attachment R).

6. Evidence Introduced at Trial

Lu's trial commenced on February 24, 2025. (R. 90: Transcript, PageID 871). The government introduced numerous exhibits during its case-in-chief, including Exhibits 13 and 22. After the government rested, Lu testified on his own behalf. (R. 96: Transcript, PageID 2058). Lu's testimony was wide-ranging, but the central theme was that the allegedly malicious code served legitimate purposes including troubleshooting and protecting Eaton's network. (*Id.,* PageID 2094-97, 2120-23, 2139-40). Lu admitted to executing the Hunshui.java program on specific dates but, while he was aware of the server crashes, he opined that his code did not cause the crashes. (*Id.,* PageID 2242, 2331, 2178, 2250). To support this, Lu claimed that he was not even logged on to the development server at the time the crashes occurred. (*Id.,* PageID 2238-39, 2242-43).

Following Lu's testimony, the Government re-called Special Agent Monica Hantz. (*Id.,* PageID 2387). In anticipation of her testimony, Special Agent Hantz prepared Exhibits 13A, 13B, and 22. Special Agent Hantz presented evidence challenging Lu's testimony regarding his computer activity. She testified that Lu received over 1,100 automated email alerts. (*Id.,* PageID

2391). A sample of those emails from August 26-28, 2019, was presented as Exhibit 13A and a graph depicting alert frequency from June to September 2019 (Exhibit 13B) contradicting his claims (*Id.,* PageID 2393-96). Agent Hantz highlighted an exponential increase in these alerts starting August 4, 2019, continuing until Lu's laptop was seized in September 2019. (*Id.,* PageID 2396-99).

Furthermore, Special Agent Hantz clarified Lu's connection to the LOUTCSDENOV3 server. On direct examination, Lu used a spreadsheet on Exhibit 40, page 57 to claim that he "did not log onto DENOV3 server on August 2, 3 and 4." (R. 96: Transcript, PageId 2187). The spreadsheet Lu presented shows only 14 connections. However, Agent Hantz testified in rebuttal that there were actually 95,000 Windows event logs linking Lu's Eaton ID to that server between August 1-7, 2019. (*Id.,* PageID 2399-2401). She explained that Lu's testimony and presentation only showed a narrow search for the server name (LOUTCSDENOV3) within these logs, leading to his misleadingly low count. (*Id.,* PageID 2401-02). Agent Hantz emphasized that a more accurate search by date, as demonstrated in Exhibit 22 for August 2, 3, 4, and 6, would reveal the extent of Lu's activity, directly refuting his implication that he was not logged on to the LOUTCSDENOV3 server on August 4, 2019. (*Id.,* PageID 2402-05).

The jury found Lu guilty. (R. 81: Verdict, PageID 818).

III. Arguments and Legal Standards

A. Rule 33 Motion for a New Trial

Lu moves this Court to grant him a new trial following the jury's unanimous verdict finding him guilty of the sole count in the indictment. Federal Rule of Criminal Procedure 33 provides that "[u]pon the defendant's motion, the court may vacate any judgment and grant a new trial if the interest of justice so requires." Fed. R. Crim. P. 33(a). The decision of whether

"the interest of justice" requires a new trial rests in the discretion of the district court judge. *See United States v. Wettstain*, 618 F.3d 577, 590 (6th Cir. 2010). "The rule does not define 'interest of justice' and the courts have had little success in trying to generalize its meaning." *United States v. Munoz*, 605 F.3d 359, 373 (6th Cir. 2010) (internal quotation marks and citation omitted). It is, however, "widely agreed that Rule 33's 'interest of justice' standard allows the grant of a new trial where substantial legal error has occurred." *Id.* (citation omitted). Any legal error that is significant enough to require reversal on appeal is an adequate ground for granting a new trial. *See Id.* (quoting with approval *United States v. Wall*, 389 F.3d 457, 474 (5th Cir. 2004)).

Rule 33 motions are disfavored, and a trial court's denial of a Rule 33 motion will be affirmed absent a clear abuse of discretion. *United States v. Willis*, 257 F.3d 636, 642 (6th Cir. 2001). "The defendant bears the burden of proving the need for a new trial and such motions should be granted sparingly and with caution." *United States v. Turner*, 995 F.2d 1357, 1364 (6th Cir. 1993). Lu alleges that the Government committed a Fed. R. Crim. P. 16 discovery violation and did not provide impeachment evidence to him until shortly before its use at trial. Typically, a movant that alleges a discovery violation must show: (1) new evidence discovered after trial; (2) that could not have been discovered earlier with due diligence; (3) that is material, and not merely cumulative or impeaching; (4) that likely would have resulted in an acquittal. *See United States v. Jones*, 399 F.3d 640, 648 (6th Cir. 2005); *United States v. O'Dell,* 805 F.2d 637, 640 (6th Cir. 1986).

B. Federal Rule of Criminal Procedure 16

Lu alleges a Fed. R. Crim. P. 16 violation because he claims that he did not receive the two rebuttal exhibits until they were provided prior to the Government's rebuttal witness

testimony. Lu cannot dispute his awareness of this data's existence well before the trial commenced on February 24, 2025. As discussed fully above, on November 2, 2022, the Government provided a discovery drive to defense which included FBI 302s detailing the issuance of a subpoena to Eaton for all of Lu's emails. (*See* Attachment O). Further, the disclosure included the subpoena itself and an FBI 302 noting the receipt of those records. (*See* Attachments P and Q). On July 19, 2024, before the initial July 2024 trial date, the Government provided the defense with its case-in-chief trial exhibits, including Exhibit 13. This exhibit was substantially identical in format and substance to the rebuttal Exhibit 13A, and contained some of the very content Lu now claims he never received (*See* Attachments R and S). Lu even referenced this material in his direct examination PowerPoint presentation (*See* Attachment T). Therefore, Lu's current assertion that he never received documents he clearly knew to exist is unconvincing.

Pursuant to Rule 16, the government must permit a defendant to inspect items in the government's control if the defendant requests such inspection and the item is material to prepare the defense. Fed. R. Crim. P. 16(a)(1)(E)(i). Materiality requires "an indication that pre-trial disclosure would have enabled the defendant to 'alter the quantum of proof in his favor'." *United States v. Dobbins*, 482 Fed.Appx. 35, 41 (unpublished) (quoting *United States v. Stevens*, 985 F.2d 1175, 1180 (2d Cir. 1993) (other citations omitted)). At the very least, Lu had notice of the existence of this data dating back to November 2, 2022, and was provided examples of the data on July 19, 2024, yet never requested to inspect them.

C. The Government Provided the Records that Lu Requested or Otherwise Made them Available for Inspection.

Lu cannot show that Exhibits 13A, 13B, and the underlying data were new evidence or that they could not have been discovered with due diligence. In his motion, Lu claims that, in

discovery, he specifically asked for the data underlying rebuttal Exhibits 13A and 13B. (R. 108: Motion, PageID 2744). He is mistaken. Lu further accuses the Government of denying three times, during the discovery process, the existence of this data, and then *mis*representing during trial that the Government had produced this data in discovery. (R. 108: Motion, PageID 2752). These accusations stem from a misunderstanding of the evidence. Therefore, a discussion of key discovery requests and communications is essential.

On January 13, 2022, Lu's previous counsel requested, among other things: Item 6, "Electrical Enovia server restart logs from *SiteScope* from January 1, 2019, to December 31, 2019, including any/all email notifications sent to users," for examination by the defense's expert. (Emphasis added) (*See* Attachment D). The government requested that Eaton review documents in its possession to see if any were responsive to the defense request. Eventually, Eaton produced three months of SiteScope records that were classified as "daily user audit logs" generated by SiteScope. These records were provided to defense. Even a cursory comparison of the SiteScope records and Exhibits 13 and 13A reveal that they are not similar. (*See* Attachments G and S). Lu was informed by Eaton that it no longer held any further documents responsive to item 6 when he issued a Criminal Rule 17 trial subpoena to them. (*See* R. 108-2: Def. Ex. F, PageID 2791). The Affidavit by Jason Koler, the Vice President and Deputy Chief Information Security Officer at Eaton, confirms that Exhibits 13 and 13A are not SiteScope records. (*See* Attachment H). Lu's assertions regarding the government's purported failure to provide certain data in discovery are based, in large, on a mischaracterization of that data.

Lu has not met his burden of establishing the materiality of the data underlying rebuttal Exhibits 13A and 13B. Criminal Rule 16 requires the government to "permit the defendant to inspect and to copy photograph books, papers, documents, data, photographs, tangible objects,

buildings or places, or copies or portions of any of these items." Fed. R. Crim. P. 16(a)(1)(e). However, "this obligation does not arise unless 'the item is within the government's possession, custody, or control and: (i) the item is material to preparing the defense; (ii) the government intends to use the item in its case-in-chief at trial; or (iii) the item was obtained from or belongs to the defendant.'" *United States v. Llanez-Garcia,* 735 F.3d 483, 493 (6th Cir. 2013) (quoting Fed. R. Crim. P. 16(a)(1)(E)).

Lu wrongly argues that this evidence was material because if he had this evidence prior to his testimony then he might not have gone to trial and pled guilty, or he would have prepared a different strategy of defense. (R. 108: Motion, PageID 2753). "It is a defendant's burden to make a prima facie showing of materiality in order to obtain disclosure of a document under Rule 16." *United States v. Dobbins*, 482 F. App'x. 35, 41 (6th Cir. 2012) (quoting *United States v. Phillip,* 948 F.2d 241, 250 (6th Cir. 1991)). The Sixth Circuit has made the following observation regarding what makes an item material to "preparing the defense:"

> Materiality under Rule 16 has not been authoritatively defined in this Circuit. However, the Supreme Court has determined that "defense" within the meaning of Rule 16 means the "defendant's response to the Government's case in chief." *United States v. Armstrong,* 517 U.S. 456, 462, 116 S.Ct. 1480, 134 L.Ed.2d 687 (1996). Therefore, the rule applies only to 'shield' claims that 'refute the Government's arguments that the defendant committed the crime charged.' . . . It follows that *information which does not counter the government's case or bolster a defense is not material "merely because the government may be able to use it to rebut a defense position*." *United States v. Stevens*, 985 F.2d 1175, 1180 (2d Cir. 1993). Rather, there must be an indication that pre-trial disclosure would have enabled the defendant to "alter the quantum of proof in his favor," not merely that a defendant would have been dissuaded from proffering easily impeachable evidence. *Id*. In assessing materiality, we consider the logical relationship between the information withheld and the issues in the case, as well as the importance of the information in light of the evidence as a whole.

United States v. Lykins, 428 F. App'x. 621, 624 (6th Cir. 2011) (emphasis added). Accord: *United States v. McCaleb*, 302 F. App'x 410, 415 (6th Cir. 2008). The *Lykins* decision is particularly relevant. Lykins was charged with being a felon in possession of a firearm. In

providing discovery, the government did not provide Lykins a picture it had of Lykins holding a gun while hunting. However, after Lykins testified that he had never hunted with a gun, the government presented the picture as rebuttal evidence. The Sixth Circuit held that the picture wasn't material to the defense because it was used to rebut a defense position. Lu's arguments that Exhibits 13A and 13B were material to his defense fly in the face of the holding in *Lykins*. These exhibits were introduced during the government's rebuttal case specifically to rebut Lu's perjurious testimony; they were not material to his defense simply because he may have chosen a different defense strategy or chosen not to proffer "easily impeachable evidence." *Id.*

D. Rebuttal Evidence Was Only Presented to Refute Lu's Perjurious Testimony

Lu asserts in his Motion for New Trial that the government's rebuttal evidence was more than just impeachment or cumulative evidence because it damaged his case extensively. Following the defense's case-in-chief, which consisted solely of Lu's testimony and his prepared PowerPoint presentation, the Government chose to offer rebuttal testimony. This rebuttal was not, as the defense suggested, merely to "respond to Mr. Lu's impactful testimony." (R. 108: Motion, PageID 2743). Instead, the Government presented it to directly refute the following falsehoods propagated by Lu:

1) Lu testified that he was *not logged into* the development server LOUTCSDENOV3 on the 26th, 27th, and 29th of August 2019, the dates reflected in Government case-in-chief Exhibit 6. Exhibit 6 depicted select dates when Lu executed the Hunshui.java program. (Exhibit 40-Slide 59 / R. 96: Transcript, PageID 2238-39, 2242-43). Lu admitted to executing the Hunshui.java program on those dates. (R. 96: Transcript, PageID 2242, 2331).

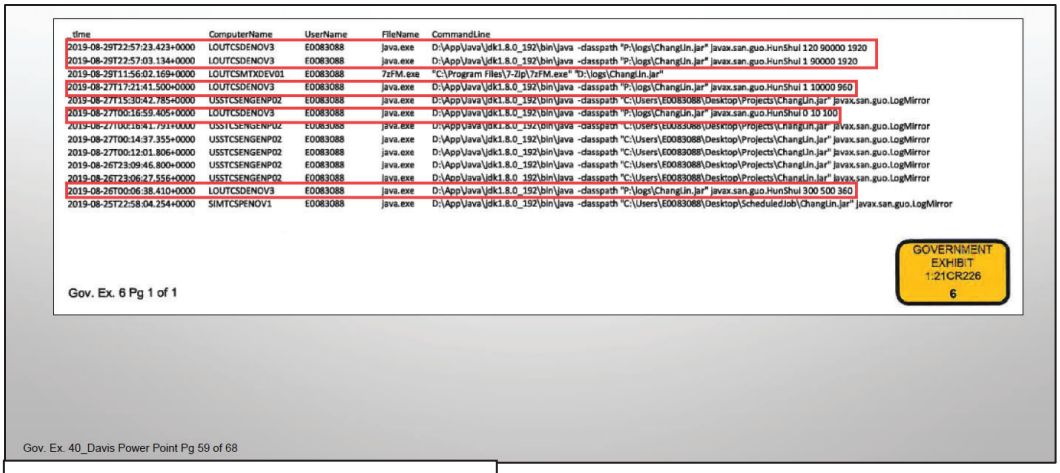


Exhibit 40-Slide 59 (Exhibit 6)

To support this claim, Lu disingenuously posited that the sampling of email alerts in Exhibit 13, containing six emails, were the totality of the system disruption alerts he received. Exhibit 13 contained alerts from the 4th, 6th, 13th, 14th, and 16th of August 2019. As a sample, the email alert for August 4, 2019 is shown below.

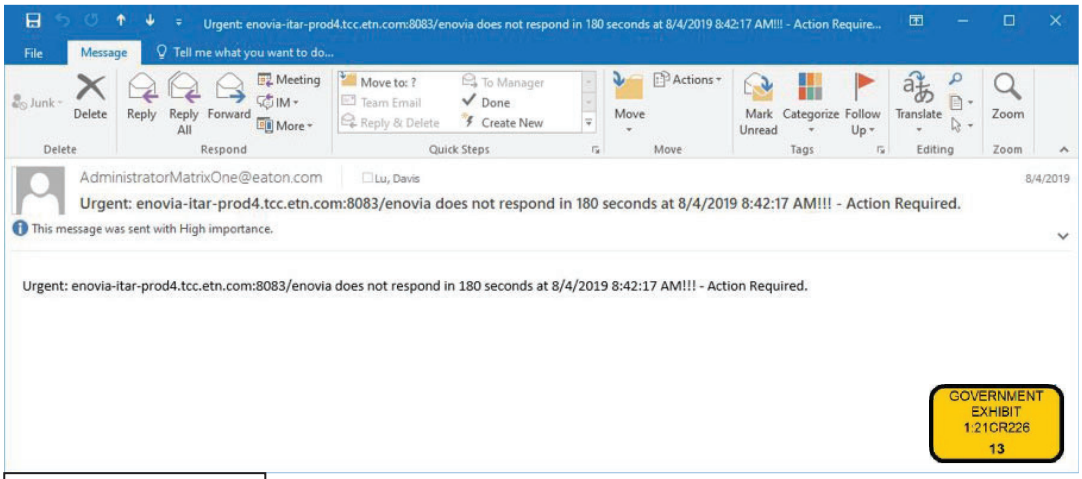


Exhibit 13, Page 1

Lu further misled the jury by conflating the information contained in Government Exhibits 6 and 13, using Exhibit 40-Slide 61, shown below.

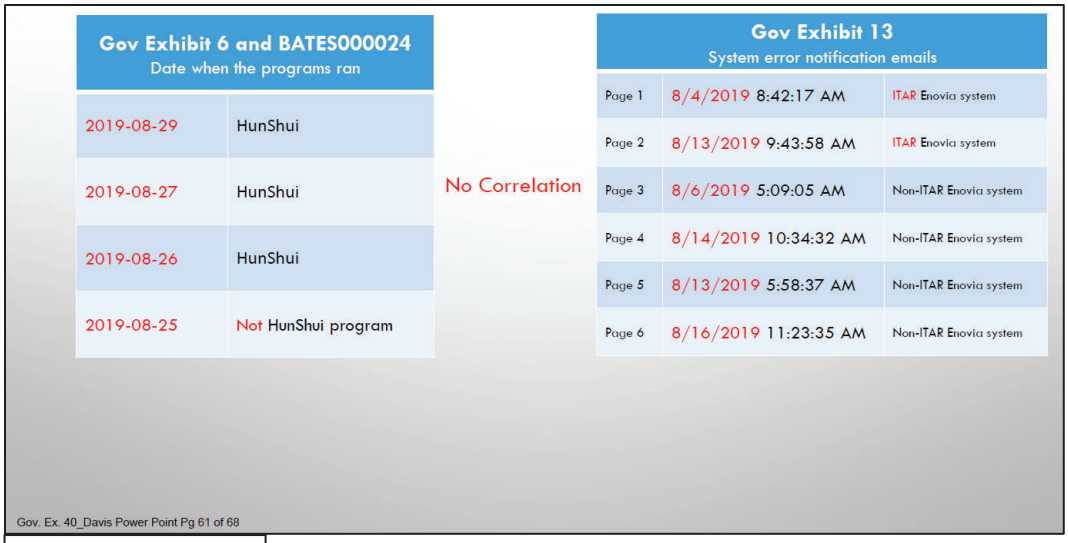


Exhibit 40-Slide 61

A. (Lu) It's clear that when my program ran 27th, 26th, and the 25th, there's no system notification error.
Also when there is a system notification error on 4th, 6th, 13th, 14th, and the 16th, my program did not run.

(R. 96: Transcript, PageID 2243).

2) Additionally, Lu misrepresented the log data in his testimony, asserting it supported his narrative of *not being logged into* the development server on August 4, 2019, the date the company first noticed the server disruptions:

B. (Lu) Yeah, because the issue was that the program must wait on the DENOV3, that particular server for the issue to appear.
And when Eaton first noticed the issue on August 4th of 2019 at 10:00 A.M., I was not on that DENOV3 server.

(R. 96: Transcript, PageID 2188-89).

To further the deception, Lu testified about and displayed to the jury Exhibit 40-Slide 57 (shown below).

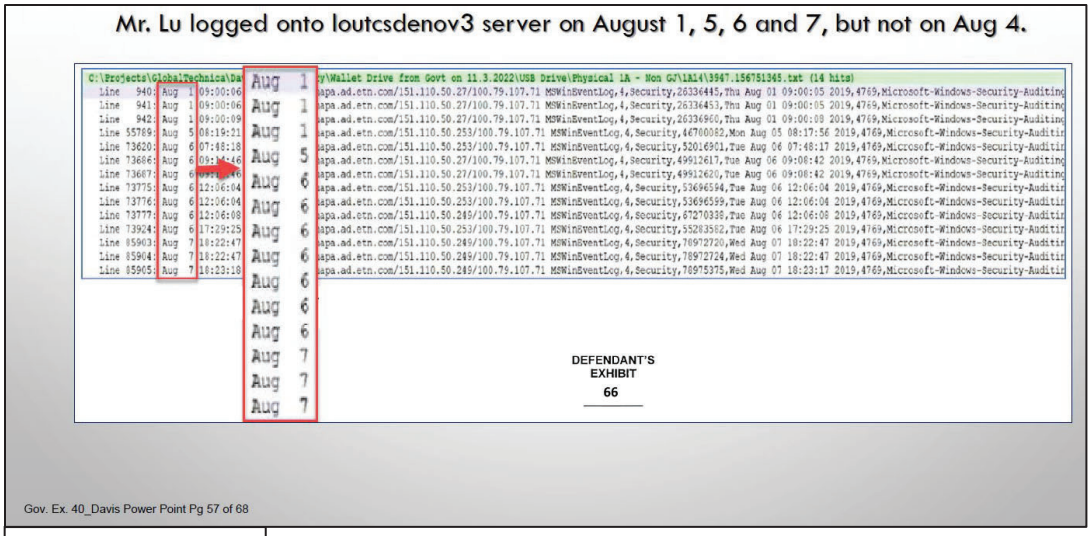


Exhibit 40-Slide 57

Q. And in this particular case, did you have occasion to review any particular server logs relative to the DENOV3 server?
A. (Lu) Yes. The application log related to me particularly and the targeted PC, the DENOV3.
Q. Okay. And is that log reflected here on the slide [Slide 57]?
A. (Lu) That is correct.

(R. 96: Transcript PageID 2186).

The fourteen entries depicted on Slide 57[1] correspond to the locations in the Windows event logs wherein the "LOUTCSDENOV3" server is named. Exhibit 40-Slide 57 depicts logons on August 1, 5, 6, and 7. Lu used this slide and corresponding testimony to support his false narrative that these were the only times he was logged in to this server. To construct this deceptive narrative, Lu deliberately limited his log search query to only entries referencing the server's name. This narrow search yielded just fourteen results, conveniently omitting over 94,900 additional log entries reflecting the server's IP address. This critical omission allowed Lu to utterly mislead

[1] Exhibit 40-Slide 57 contains excerpts from fourteen entries, starting with entry line 940 and ending with entry line 85905.

> the jury, especially since Lu's malicious code was triggered by the IP address, not the server name.
>
> However, if the request came from DENOV3, *specifically two IP addresses that were associated with DENOV3* at different points in time, then the program -- the IPFilter would erase its list, and then check its list, and then check its list again over and over and over again until all available processes were consumed and the server was no longer responding to more requests from IPFilter or, more importantly, any other request from any user in that affected application server. (Emphasis added)
>
> (R. 93: Transcript, PageID 1476).

Thus, the rebuttal testimony and exhibits presented by Special Agent Hantz directly contradicted Lu's claims regarding his limited computer activity and server connections. The testimony and the associated exhibits 13A, 13B, and 22 directly refuted and discredited Lu's prior testimony. Specifically, the testimony demonstrated that Lu was aware of, and received a significant number of, automated email alerts, contradicting any claims by Lu that he was unaware or received a negligible number of emails. Exhibits 13A and 13B provided tangible evidence of these alerts and their increasing frequency. The rebuttal evidence also exposed Lu's testimony regarding his server connections as misleading and incomplete. By detailing the 95,000 Windows event logs and explaining how Lu's search method yielded a deceptively low number of 14 connections, the government demonstrated that Lu deliberately misrepresented the extent of his activity. Rebuttal Exhibit 22 further solidified this by showing a more accurate accounting of his activity on key dates, directly challenging Lu's implication that he was not connected to the server on August 4, 2019. The rebuttal testimony thus ensured that the jury received a complete and accurate picture of the facts, directly challenging Lu's credibility and the narrative he had presented.

E. The Government's Rebuttal Evidence Directly Refuted Lu's Misleading Testimony

In his motion for new trial, Lu attacked the Government's use of Exhibits 13A and 13B during Special Agent Hantz's rebuttal testimony, claiming the government offered the same to "evince *additional* times when Mr. Lu's program had run . . . that did align with the dates of system error notifications, evinced in Exhibit 22." (R. 97: Motion, PageID 2744). A discussion of rebuttal Exhibit 22 is necessary before responding further to Lu's complaints about rebuttal Exhibits 13A and 13B.

Rebuttal Exhibit 22 is an excerpt from the Windows event logs.[2] The logs were provided to the defense in discovery. Lu even used excerpts from the Windows event logs during his testimony and displayed those excerpts in Exhibit 40, specifically Slide 57. (Exhibit 40-Slide 57 / R. 96: Transcript, PageID 2186-89).[3] Slide 57 appears to display the results of Lu's search of these logs (file name 3947.156751345).

In his Declaration attached to the defense's motion for new trial, Mr. Nemecek seemingly cast aspersions on the production by the government of the Windows event logs, contending that it "*purportedly* formed the basis of Exhibit 22" and "is a plain text file, with *no formatting*." Mr. Nemecek further complained that "[w]hen converted to PDF, it is 15,502 pages long." (emphasis added) (R: 108-2: Motion Attachment, PageID 2772).

[2] A Windows event log is a centralized logging service in Microsoft Windows operating systems that records significant event that occur on the device. https://learn.microsoft.com/en-us/windows/win32/eventlog/event-logging

[3] Defense exhibits MMMM, 70, and 71 were excerpts from the Windows event logs.

However, when the Windows event logs are opened in Notepad++ and "wrapped,"[4] the data was very readable, organized, and appeared as follows (see Image-1 below showing the first 5 entries):

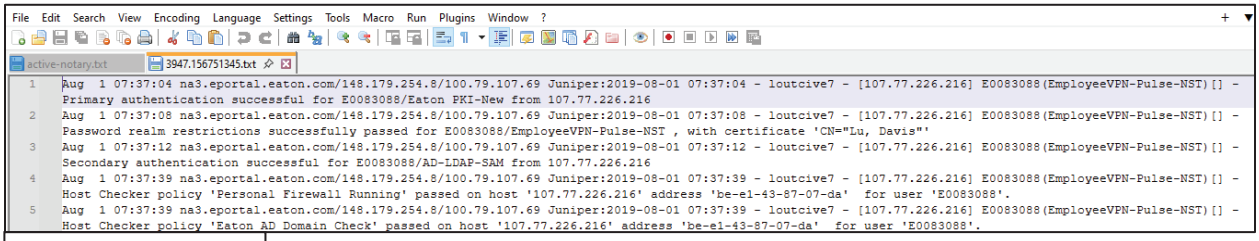


Image-1

The Windows event logs consisted of 95,000 entries, starting on August 1, 2019 at 7:37:04, and ending on August 7, 2019 at 17:17:01. In her case-in-chief testimony, Special Agent Hantz referenced a "spreadsheet" which indicated that Lu was logged into the server on August 4, 2019.

> **Q.** Are you aware of whether or not Davis Lu was on the Enovia server on August 4th, 2019?
> **A. Special Agent Hantz** So based on the analysis conducted, there was spreadsheets indicating that his user ID was logged in in the servers, yes.
> **Q.** All right. And that's the information that we've reviewed here in this case?
> **A. Special Agent Hantz** That's correct.
>
> (R. 95: Transcript PageID 1984).

When Special Agent Hantz spoke of a "spreadsheet," she was referring to the Windows event logs, which she subsequently explained in her rebuttal testimony. The defense's criticism of the formatting and volume of the Windows event logs is a red herring. It should be noted that these logs can be easily searched (see the search tab in Image-1 above: third tab from the top left). Special Agent Hantz replicated the defense's search of the Windows event logs using the query

[4] Notepad++ is a free and open-source text and source code editor for Windows. https://notepad-plus-plus.org/ Wrapping text is when a block of text is formatted so that it fits within a designated area, like a page, window, or cell.

LOUTCSDENOV3 and obtained the same fourteen entries displayed in the slide deck Lu presented and testified about, specifically Exhibit 40-Slide 57. (R. 97: Transcript PageID 2400-01). Image-2 below is a screenshot of a "Find" dialog box for such a search of the logs, reflecting 14 "hits" or matches.

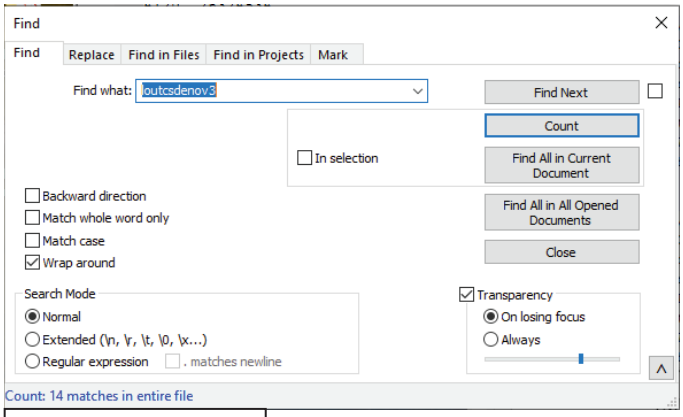
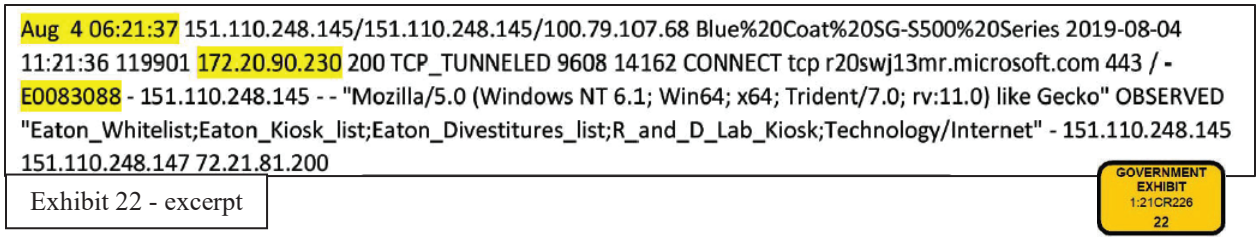


Image-2

Lu's counsel never indicated any issue with viewing the event logs prior to trial and it is apparent from Lu's testimony that he created Exhibit 40-Slide 57 by reviewing the totality of the Windows event logs (file name 3947.156751345) and conducting a search for LOUTCSDENOV3. (R. 96: Transcript, PageID 2186).

During her rebuttal testimony, Special Agent Hantz confirmed that the 95,000 entries in the Windows event logs were all attributed to Lu's development server, either by the server name LOUTCSDENOV3 or its IP address. (R. 97: Transcript, PageID 2401-02). In preparation for her rebuttal testimony, Special Agent Hantz conducted a search of the Windows event logs for events evidencing Lu being logged on to the server. From that search she selected four examples – dated August 2, 3, 4, and 6, 2019 – and created rebuttal Exhibit 22. (*Id.,* PageID 2404-05). Below is one of the examples selected, from Exhibit 22, with the IP address, the date, and Lu's employee ID number highlighted.


Aug 4 06:21:37 151.110.248.145/151.110.248.145/100.79.107.68 Blue%20Coat%20SG-S500%20Series 2019-08-04 11:21:36 119901 172.20.90.230 200 TCP_TUNNELED 9608 14162 CONNECT tcp r20swj13mr.microsoft.com 443 / - E0083088 - 151.110.248.145 - - "Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko" OBSERVED "Eaton_Whitelist;Eaton_Kiosk_list;Eaton_Divestitures_list;R_and_D_Lab_Kiosk;Technology/Internet" - 151.110.248.145 151.110.248.147 72.21.81.200

GOVERNMENT EXHIBIT 1:21CR226 22

Exhibit 22 - excerpt

Rebuttal Exhibit 22 neither depicted nor involved email alert notifications. Exhibit 22 did not show when Lu ran his malware. Thus, the defense's representation that the government offered rebuttal Exhibits 13A and 13B to "evince additional times when Mr. Lu's program had run . . . *that did align with the dates of system error notifications, evinced in Exhibit 22,*" is entirely nonsensical. (emphasis added) (R. 108: Motion, PageID 2744). Exhibit 22 simply refutes Lu's testimony that he was not logged in on August 4, 2019, and counters Lu's Exhibit 40-Slide 57.

To preface the government's use of its rebuttal Exhibits 13A and 13B, Special Agent Hantz recounted Lu's case-in-chief testimony wherein he compared and contrasted the dates in Government Exhibit 13 (six email alerts between August 4, 2019 and August 16, 2019) and the dates in Government Exhibit 6 (showing Lu's execution of HunShui between August 26, 2019 and August 29, 2019). Lu denied that any system crash occurred when he ran HunShui. (R. 97: Transcript, PageID 2388-91).

In anticipation of her rebuttal testimony, Special Agent Hantz assembled a new packet of sample email alert notifications, labeled Government Exhibit 13A. Rebuttal Exhibit 13A was similar in substance and formatting to case-in-chief Exhibit 13, and consisted of 6 email alert notifications for the 26th, 27th, and 29th of August 2019. (Exhibit 13A / R. 97: Transcript, PageID 2394-96). She also created Government Exhibit 13B—time-series line graph—summarizing the volume of email alerts Lu received per day between June 26, 2019, and September 5, 2019, the date he surrendered his laptop. (Exhibit 13B / R. 97: Transcript, PageID

2391, 2393). Exhibits 13A, 13B and 22 were created after Mr. Lu's direct examination which ended at 4:54 p.m. on March 4, 2025, and before Special Agent Hantz' rebuttal testimony which started the following day at 2:00 p.m. (R. 96: Transcript, PageID 2253, 2387).

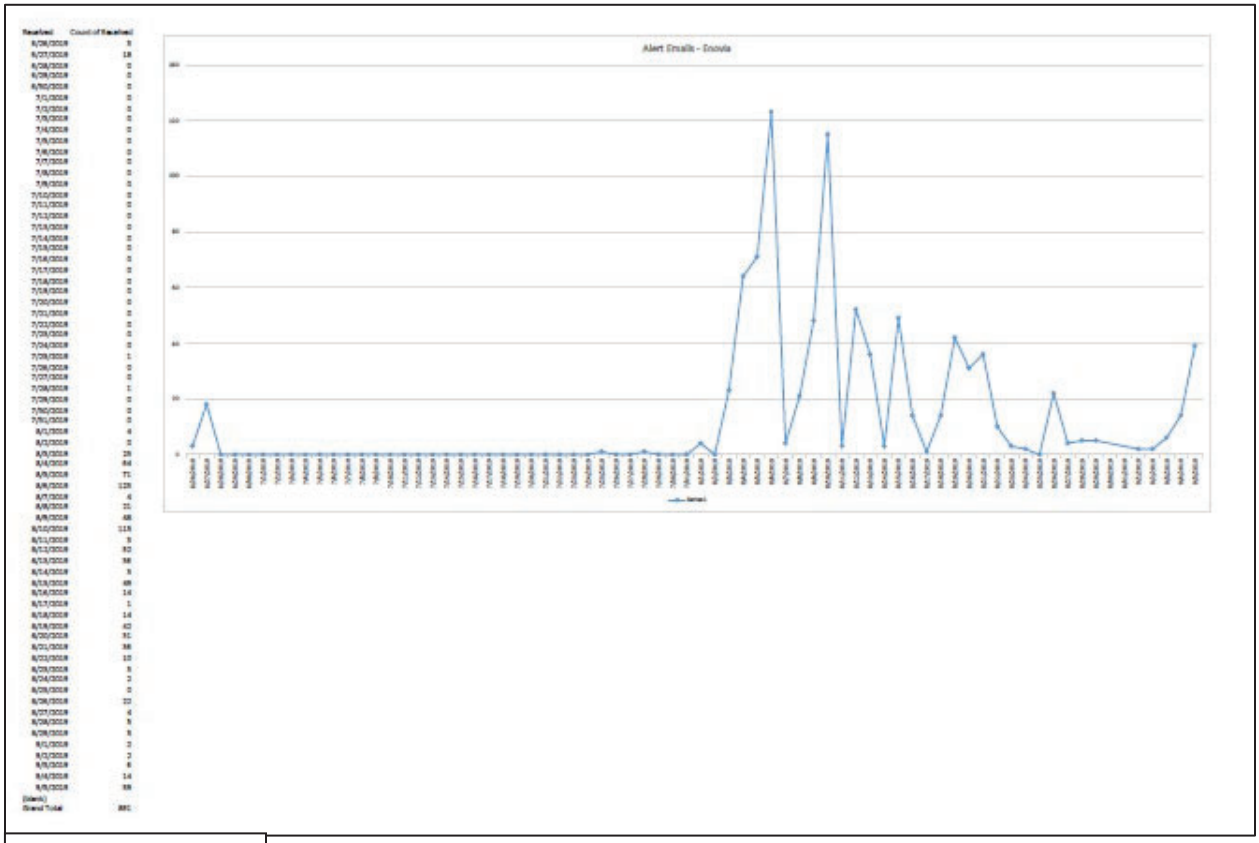


Exhibit 13B

The entries on the left-hand side of the line graph revealed the number of non-ITAR email alert notifications received per day, culminating with a grand total of alerts. Although Special Agent Hantz testified there were approximately 840 non-ITAR email alerts, her line graph more accurately revealed a grand total of 891 non-ITAR email alerts (see Exhibit 22, Enlarged Image below, showing the final 11 lines). (Exhibit 13B / R. 97: Transcript, PageID 2391).

8/26/2019	22
8/27/2019	4
8/28/2019	5
8/29/2019	5
9/1/2019	2
9/2/2019	2
9/3/2019	6
9/4/2019	14
9/5/2019	39
(blank)	
Grand Total	891

Exhibit 22, Enlarged Image

In its motion for new trial, the defense repeatedly cried "surprise" and "ambush." However, it is unconvincing to believe that Lu, who was noticed as his own technical expert witness (subject matter: computer coding and functionality); who was himself the recipient of approximately 1400 relevant email alert notifications; and whose job responsibilities while employed at Eaton included resolving issues corresponding to such email alert notifications, was in any way surprised.

During his testimony, Lu made numerous concessions to the government's evidence. He admitted under oath that he wrote and executed the code. (R. 96: Transcript, PageID 2077, 2093-94 / R. 97: Transcript, PageID 2310). He conceded that he knew the company's systems were repeatedly crashing in August and September 2019. (R. 97: Transcript, PageID 2299). He confessed to receiving automated system email alerts about the disruptions, albeit disagreeing with the actual number of email alerts received. (*Id.,* PageID 2298). He acknowledged that the email alerts compiled in case-in-chief Exhibit 13 were merely *examples*, not a comprehensive list.

> **Q.** And, in fact, you knew the servers were hanging, didn't you?
> **A. (Lu)** Yeah, I was working on it, yeah.
> **Q.** The question was, though, you knew the servers were hanging, didn't you?
> **A. (Lu)** That is correct.
> **Q.** Both because you were getting e-mail alerts, and also because you were talking to your co-workers about it; isn't that right?
> **A. (Lu)** That is correct.

(R. 97: Transcript, PageID 2299).

Q. There was a dramatic increase in servers hanging started on August 4th of 2019; isn't that true?
A. (Lu) The dramatic increase from a time before that.
Q. You received the alerts when there was a server hang; isn't that true?
A. (Lu) That is correct.
Q. And so the e-mails that the Government has shown examples of *are examples of the e-mails that you received* when there's an issue with a server; isn't that right?
A. (Lu) *Yes.*
Q. You didn't receive a single e-mail indicating an issue with the server in all of July of 2019, did you?
A. (Lu) I do not recall.
Q. But you did receive hundreds of e-mails indicating issues with the server in August of 2019, didn't you?
A. (Lu) I don't believe it is hundreds.
Q. You don't believe you received 1400 e-mail alerts indicating issues with the server in August and September of 2019?
A. (Lu) I don't believe the number is 1400, no.

(emphasis added) (*Id.,* PageID 2297-98).

F. Lu's Legitimate Defensive Strategies Were Not Precluded, Thus Lu Cannot Establish Materiality

Since Lu was indicted, the defense has consistently asserted that Lu lacked the requisite intent to write or execute malicious code, that Lu's code had a legitimate purpose, and that Lu's code was not the proximate cause of any system failures. (R. 97: Transcript, PageID 2251, 2250). In an attempt to dispute causation, Lu posited that he was not logged into the development server LOUTCSDENOV3 at the time of the system failures, attributing these failures to improper deployment or insufficient remediation attempts by other Eaton employees. The assertion regarding Lu's login status will be addressed subsequently. Concerning the latter point—the misattribution of system failures—Lu presented a slide from his PowerPoint presentation. Although the majority of the slides were presented to the jury and relied upon during Lu's case-in-chief direct examination, the complete PowerPoint presentation was admitted

for record purposes as Government Exhibit 40 and was not provided to the jury during its deliberations. Specifically, data from Exhibit 40-Slide 23, shown below, was employed by Lu to accuse other Eaton employees of improper deployment.

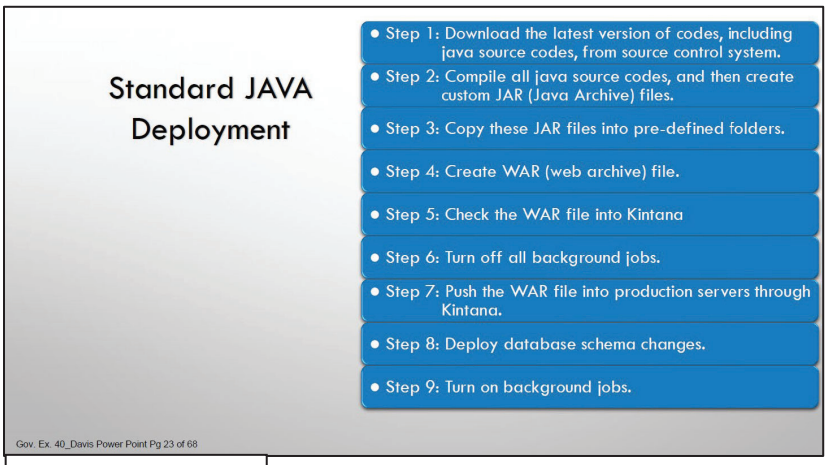


Exhibit 40-Slide 23

Lu's ability to pursue his lack of *mens rea* and legitimately purposed code defenses was not precluded by the rebuttal testimony and evidence; neither was his ability to pursue his improper deployment by others defense, at least regarding certain of the malware. Of note, the defense of improper deployment by others was not applicable to Lu's IsDLEnabledInAD malware. Lu enabled the execution of this code regardless of how deployment occurred. Upon Lu's termination, the company's standard procedure of removing his active directory credentials triggered the kill switch code[5] Lu had secretly implemented. This code, designed to prevent any unauthorized system login, remained active for up to a year after Lu's departure, effectively locking out all users. (R. 92: Transcript, PageID 1393-98, 1428-33, 1437-39). Lu admitted

[5] A kill switch code is a hidden or intentionally implemented piece of programming designed to remotely disable functionality, delete data, or shut down a system upon a specific trigger. https://amplitude.com/explore/experiment/what-is-a-kill-switch-in-software-development In this case the trigger was that of the login servlet checked the active directory and found that Lu's employee number was no longer active, it would not permit any user to login. (R. 92: Transcript, PageID 1429).

writing and enabling this code. (R. 96: Transcript, PageID 2126). It is uncontroverted that rebuttal Exhibits 13A, 13B, and 22 were categorically unrelated to Lu's IsDLEnabledInAD malware. Lu would not have received any email alert notifications (Exhibit 13A and 13B) related to the disruptions caused by IsDLEnabledInAD or have been logged into the system (Exhibit 22) during the execution of IsDLEnabledInAD, since that malware impacted the system only after Lu's termination when his credentials were removed from the active directory. The government posits that this malware presented overwhelming evidence of Lu's criminal intent, rendering his "legitimate purpose" defense baseless, discrediting the misattribution argument, and utterly decimating his credibility.

Thus, while the rebuttal testimony and evidence did not preclude Lu's ability to claim a lack of *mens rea*, the evidence presented during the government's case-in-chief was replete with evidence of Lu's criminal intent. The overwhelming evidence establishing Lu's criminal intent undermined his credibility as a witness. The trial evidence demonstrated that after the creation and execution of any of the malicious code, Lu elected not to upload it to the company's code repository site, a decision that further concealed the code and frustrated his colleagues' investigation and remediation efforts. (R. 92: Transcript, PageID 1357, 1396, 1433, 1500 / R. 93: Transcript, PageID 1602, 1617 / R. 94: Transcript, PageID 1732-34, 1752-53, 1823. Most if not all of the malicious code was found in Lu's possession on his laptop. Witnesses confirmed that the code was in fact malicious in nature, and Lu continued to modify the malicious nature of the code to thwart the investigative efforts of his colleagues. R. 92-93: Transcript, PageID 1413-14, 1437-38, 1473, 1490-95, 1540, 1546, 1571. The act of writing and executing malicious code, as brought out through the case-in-chief witnesses and exhibits, inherently contradicted Lu's subsequent testimony that the code had a legitimate business purpose. The testimony of the

significant server disruptions caused by the various code written by Lu served as strong circumstantial evidence against Lu's claim of a legitimate purpose. Matt Rose testified as to the amount of time spent by Eaton employees to remediate the negative impact of Lu's code.

> **A. Matt Rose** . . . one [server] would hang, and then within minutes, perhaps two hours, maybe a second one would hang. And if we waited long enough, perhaps a third one. And had we waited long enough, you know, you get the idea. They would generally fail one at a time. Until they were restarted, you know, they would stay hung.
>
> (R. 92: Transcript, PageID 1361-62).
>
> **A. Matt Rose** I spent most of August troubleshooting and diagnosing and trying to get to the bottom of this problem.
>
> (*Id.,* PageID 1365).
>
> **A. Matt Rose** we began what was -- what turned into a very large remediation effort to identify and repair all of those affected programs.
> Q. Describe that, please.
> **A. Matt Rose** Well, it was a -- it was about 12 to 18 months, I think, to fully remediate every program that was – that was affected.
>
> (*Id.,* PageID 1397).

G. The Interest of Justice Does Not Warrant A New Trial Because Lu Does Not Have a Constitutional Right to Present a Defense Based On Deception and Perjury

In his motion for new trial, Lu complained that the harm suffered by Lu included him getting "*caught* in an apparent deception by the jury." (emphasis added) (R. 108: Motion, PageID 2753). Lu has only himself to blame for pursuing a defensive strategy based on misrepresentations and lies. While a criminal defendant possesses a fundamental constitutional right to present a defense, this right is not without crucial limitations. It does not extend to the presentation of false testimony or evidence, as the integrity of the judicial process outweighs any perceived right to deceive the court. The Supreme Court has definitively ruled that a criminal defendant's constitutional rights do not encompass the right to present perjured testimony. *Nix v.*

Whiteside, 475 U.S. 157, 173 (1986) ("whatever the scope of a constitutional right to testify, it is elementary that such a right does not extend to testifying falsely").

The Sixth Amendment, often interpreted in conjunction with the Due Process Clause of the Fifth and Fourteenth Amendments, guarantees criminal defendants "a meaningful opportunity to present a complete defense." This fundamental right is a cornerstone of the American adversarial system, ensuring fairness and due process in criminal prosecutions. However, this right does not extend to presenting perjurious testimony. Lu seeks to do just that when he writes that, under different circumstances, Lu's testimony may have "focused on other weak points in the Government's case, and not on an argument that the evidence directly refuted." (R. 108: Motion, PageID 2738). Later in his motion, Lu asserts: "If [Mr. Lu] had known about the [Exhibit 13A and 13B Files], he—and his counsel—would not have been caught in an apparent deception by the jury during deliberations." (*Id.,* PageID 2753, paraphrasing *United States v. Lee*, 573 F.3d 155 (3d Cir. 2009)). The thrust of his argument appears to be an attempt to avoid being *caught* in perjury, or for the opportunity to have perjured himself differently had he known the Government was ready to challenge him with the data contained in its rebuttal exhibits. Lu should be precluded from asserting any claim of harm, as such a claim directly arose from the demonstrable failure of his defensive strategy to obscure or misrepresent the truth during trial, thereby exposing his deception and perjury. To permit such a claim would countenance a defendant benefiting from their own mendacity and undermining the integrity of these proceedings. It certainly cannot be the basis of a finding of injustice justifying a new trial.

IV. Conclusion

During trial, Lu engaged in a calculated and dishonest attempt to deceive the court and the jury, and to obstruct justice. His perjured testimony was a strategic fabrication, tailoring his testimony to just the excerpts of evidence the government selected as exhibits to submit to the jury. Lu made a conscious decision to ignore what he knew to be true, and to present, through his testimony, a wholly false narrative. He utterly fails in his motion for new trial to establish (1) that Exhibits 13A and 13B, or more simply, the email alert notifications, constituted new evidence; (2) that they could not have been discovered earlier; (3) that they were material, and not merely cumulative or impeaching; and finally, (4) that when considering the overwhelming evidence of guilt presented during the case-in-chief, that precluding the admission of Exhibits

13A and 13B would likely have resulted in an acquittal. Therefore, Lu's motion should be denied.

Respectfully submitted,

CAROL M. SKUTNIK
Acting United States Attorney

By: /s/ Daniel J. Riedl

Daniel J. Riedl (OH: 0076798)
Brian Deckert (OH: 0071220)
Assistant United States Attorneys
United States Court House
801 West Superior Avenue, Suite 400
Cleveland, OH 44113
(216) 622-3669/3873
(216) 685-2378 (facsimile)
Daniel.Riedl@usdoj.gov
Brian.Deckert@usdoj.gov

/s/ Candina S. Heath

Candina S. Heath (TX #09347450)
Senior Counsel
U.S. Department of Justice Criminal Division
Computer Crime & Intellectual Property Section
John C. Keeney Building, Suite 600
Washington, DC 20530
(202) 923-5211
Email: Candina.Heath2@usdoj.gov